FREQUENCY SENSOR FOR SIDE-CHANNEL ATTACK

BACKGROUND

[0001] Field

[0002] The present disclosure relates generally to cryptographic systems, and more particularly, to a frequency sensor that may be used to attempt to determine if a side-channel attack on the cryptographic attack is occurring.

[0003] Background

[0004] FIG. **1** is a diagram illustrating an example cryptographic system **100**. The cryptographic system **100** may include a cryptographic algorithm for encrypting data, decrypting data, or both. For example, the cryptographic system **100** may generally take inputs **104** and encrypt those inputs to produce an encrypted output **106**. Encryption is the process of encoding messages or information in such a way that, if the encryption is successful, only authorized parties are able to read the encrypted message. Encryption may deny a message's content from those who may intercept a message.

[0005] When the cryptographic system **100** is encrypting data, the inputs **104** may be referred to as plaintext. The inputs **104** to the cryptographic system **100**, when encrypting are generally unencrypted data. The data has generally not been previously encrypted. However, in some cases, a system may further encrypt a previously encrypted message. The inputs **104**, e.g., plaintext, may be encrypted using the encryption algorithm **102** that is part of the cryptographic system **100**. The cryptographic system **100** may generate the output **106**. The output **106** of the cryptographic system **102** may be an encrypted version of the input **104**. The encrypted output **106** may be referred to as "ciphertext," e.g., when the cryptographic system is encrypting data. Generally, if the encryption scheme is successful, the encrypted output or ciphertext may only be read if decrypted.

[0006] Conversely, when the cryptographic system **100** is decrypting data, the inputs **104** may be referred to as encrypted data or ciphertext. The inputs **104** to the cryptographic system **100**, when decrypting are generally plain unencrypted data, i.e., plaintext. The data may generally not have been encrypted multiple times. However, in some cases, a system may further encrypt a message such that the data is encrypted multiple times. The inputs **104**, e.g., ciphertext, may be decrypted using the encryption algorithm **102** that is part of the cryptographic system **100**. The cryptographic system **100** may generate the output **106**. The output **106** of the cryptographic system **102** may be a decrypted version of the input **104**.

[0007] Depending on the encryption scheme, a key may be needed to convert the encrypted output or ciphertext back to the plaintext. The key may be a random or pseudo random sequence of bits used to encrypt the data, decrypt the data, or both. An authorized recipient, e.g., a recipient rightfully having the proper key, may generally be able to decrypt the message with the key. Those not authorized to access the encrypted information may not be provided with the proper key and generally may not be able to decrypt the information or may not be able to decrypt the information without dedicating a large number of resources to breaking the encryption.

[0008] Generally, encryption systems are used to protect sensitive information. This sensitive information may include voice communication and data communication. The data may be sensitive data such as banking records, PIN numbers, social security numbers, and other personal information. Data having monetary value, such as music or videos may also be encrypted so that the music or videos are only accessible to those who may have purchased such content. (This assumes that the encryption for this content has not been broken.)

[0009] In some instances, people may use various side-channel attacks on the cryptographic system **100** in an attempt to gain access to information on the cryptographic system **100**, such as the key used to encrypt and decrypt data. In cryptography, a side-channel attack is any attack based on information gained from the physical implementation of a cryptosystem. The side-channel attack may modify various conditions under which the cryptographic system operates to try to gain information, such as the key being used. A side channel attack may be contrasted with a brute attack. A brute-force attack is a cryptanalytic attack that may, in theory, be used against any encrypted data having a finite cryptographic key. The brute force attack may try multiple keys in an attempt to decrypt encrypted data. For example, the brute-force attack may systematically go through the keys. In some instances, knowledge of the data being encrypted may be used to eliminate some number of potential keys in a brute-force attack.

[0010] Examples of side-channel attacks include, but are not necessarily limited to attacks manipulating timing, voltage, temperature, and clock inputs, to name a few. When completing a side channel attack, the attacker may monitor timing, outputs, fault outputs, power consumption, electromagnetic emissions, or other outputs of the cryptographic system **102** under attack.

[0011] It may be useful to monitor for one or more aspects of a side-channel attack.

SUMMARY

[0012] In an aspect of the disclosure, a method, a computer program product, and an apparatus are provided. A method, an apparatus, and a computer program product for wireless communication are provided. The apparatus may be used for detecting an incorrect clock frequency. In one example, the apparatus includes a first circuit configured to compare a clock signal period to a delay period. Additionally, in one example, the apparatus includes a second circuit configured to output a first signal. The period of the first signal may be double the clock signal period when the clock signal period is greater than the delay period. The apparatus may, in one example, also include a third circuit configured to output a second signal. The period of the second signal may be smaller than the clock signal period when the clock signal period is smaller than the delay period.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. **1** is a diagram illustrating an example cryptographic system.

[0014] FIG. **2** is a diagram illustrating an example implementation of a frequency sensor that may be used to determine if some aspects of a side-channel attack are occurring.

[0015] FIG. **3** is a timing diagram illustrating an example of signal timing for a frequency sensor illustrated in FIG. **2**.